



Whistler Design Preview

April 20 & 21



Beyond Windows 2000

Security

Directions...

Praerit Garg
Windows Security
Microsoft Corporation

Topics

- **Beyond Windows 2000 Themes**
- **Authentication**
- **Data Protection**
- **Security Management**
- **Applications and access control**
- **Large scale PKI deployment**
- **Common Criteria Evaluation**

“Whistler” Themes

- **Build on Windows 2000 platform foundation**
- **Improve end user's security experience**
- **Provide flexible and high perf. access control to applications**
- **Continue to improve security management & monitoring**
- **Support large-scale deployment of PKI enabled applications**

Security for Whistler Personal

- **Update the user security model for consumer use**
- **Personal firewall with stateful inspection by default**
- **Personalized logon UI**
- **Administrator used only for safe-mode boots**
- **New users and passwords applet with support for multiple credentials**

End User SSO

Experience

- **Credential Manager**
 - Simplify user logon experience
 - Multiple intranet and Internet services \Leftrightarrow Multiple credentials
 - Transparent use, automatic handling of different credentials - passwords, certificate/private keys, ...
 - Per-user encrypted store
 - Common end-user UI
- **Active Directory support for Digest Authentication protocol**

Smart cards for Administrators

- **Enable use of smart cards for administrative operations**
- **Smart card credentials to “Map network drive”**
- **Runas support for smart card**
- **Automatic password management for users that must logon with smart card**
- **Smart card credentials for terminal server sessions**

Using Encrypted Files

- Enable more ways to use encrypted files easily
 - Enable sharing of encrypted files
 - Encrypted client side cache
- Performance enhancements of EFS driver
- Support kernel-mode FIPS-compliant cryptography
- Simplify standalone recovery model
- Looking at ways to support encrypted files on Web drives

Security Management

- **Remote Security Configuration Tools enabled using WMI**
 - Remote configuration, analysis, and reporting capabilities
- **Secure Server Roles - Web, File/Print, Domain Controllers**
- **UI to show effective permissions for an individual user**
- **Active Directory access management**
 - Delegation wizard improvements
 - Reset of permissions on Oll subtree

Security Management

- **Better control of distributed security infrastructure**
 - **Enforcement of SID validity across trust links**
 - **High availability offline logon capability for clusters**
 - **Looking at ways to enable cross-forest authentication**
 - **Kerberos and NTLM**

Security Monitoring

- WMI enabled trust monitoring and self healing
- Auditing file I/O operations (Read/Write)
- Increased auditing in Certificate Server, Time server, others
- Plumbing work for WMI based audit infrastructure (coming soon...)
 - Extensible, flexible, smarter, scalable, complete

Improve application server security

- **Least-privilege context for services**
 - **Local System, Local Service, Network Service, Domain service**
 - **Improved robustness and security**
- **Application-level access check mechanism**
 - **Support for application-defined business rules and dynamic groups**
 - **High performance for distributed authorization with central control**

Large Scale PKI Deployments

- **Interoperability**
 - **Cross certificates for Bridge CA and Entrust interoperability**
 - **New cert request message types (CMC)**
- **CA management**
 - **Better role separation, increased granularity of operational roles**
- **Enrollment Agents for ECA delegation**
- **Delta CRLs for increased CRL**

Windows 2000 Common Criteria

Evaluation Formal evaluation of Windows 2000 security mechanisms

- **Common Criteria as evaluation process for all future evaluations**
 - **Security Target, Operating System Protection Profile (CAPP)**
- **Subsystem by subsystem analysis and requirements verification**
- **Correspondence test matrix**

For More Information

- **White papers**
 - <http://www.microsoft.com/windows2000/library>
 - **Microsoft Windows 2000 Distributed Security Services**
 - **Next-Generation Windows 2000 Directory Services**
 - **Windows 2000 Encrypting File System**
 - **Windows 2000 Security Configuration Tool Set**
- **Windows 2000 Server Resource Kit**
 - **Distributed Systems Guide**
- **Microsoft Security Advisor**

Where do you want to go today?®

Microsoft®